SPECTRUM Hinweise

Unabhängiger KANZLEI Systempartner

Juli 2025

Datenschutz & Microsoft CoPilot

Für die Einhaltung der europäischen Datenschutz-Empfehlungen zur Nutzung von Microsoft 365 hat SPECTRUM bei der Installation von Microsoft 365 diverse Sicherheits-Einstellungen vorgenommen – siehe separaten SPECTRUM-Hinweis „Hinweise zu den technischen Einstellungen bei der Installation durch SPECTRUM von Microsoft 365 Business Premium auf SPECTRUM-ASP-Systemen und generelle Sicherheitshinweise beim Einsatz von Microsoft 365“.

Für die Freigabe von Microsoft 365 Copilot muss in den M365-Einstellungen aber zwingend die Option „Verbundene Erfahrungen mit Inhalten“ in den Office-Einstellungen aktiviert werden. Hinweis: Copilot ist in allen Office-Anwendungen integriert (u.a. Outlook, Excel, Word und Teams).

Dies bedeutet, dass dann Ihre Microsoft-M365-Umgebung nicht mehr DSGVO-konform eingerichtet ist!

(Hinweis: bei der Einrichtung von M365 haben wir für Sie u.a. zahlreiche sog. „Nach-Hause-Telefonier-Funktionen“ deaktiviert, damit Ihr System datenschutzrechtlich maximal geschützt bleibt. Diese Einstellungen müssen beim Einsatz von MS-Copilot wieder deaktiviert werden.)

Ein falsch gesetztes Berechtigungsniveau kann dazu führen, dass sensible Daten durch Microsoft Copilot unbeabsichtigt offengelegt werden.

Daher ist eine gründliche Rechteprüfung im Vorfeld zwingend erforderlich. Jeder Nutzer, auch die, für die keine Copilot-Lizenz aktiviert werden soll, muss die freigegebenen Dokumente in Teams und OneDrive prüfen.

- Denn Copilot greift auf **alle** Daten zu, auf die der Benutzer innerhalb Ihrer Organisation Zugriff hat. Dies gilt natürlich auch, wenn eine Datei versehentlich für diesen Benutzer freigegeben wurde. Das kann z.B. mal passieren, wenn man ein Dokument in OneDrive speichert und hier nur einer Person zugänglich machen wollte, aber aus Versehen für alle freigibt. Im besten Falle findet diese Datei niemand Unbefugtes, Copilot aber bei der richtigen Fragestellung schon.
- Mit Copilot lassen sich auf Basis der vorhandenen Daten verschiedene Auswertungen durchführen, die für sich genommen eine eigene Rechtsgrundlage benötigen. Mit dem automatischen Transkribieren von Teams-Calls können z.B. Inhalte aus Videokonferenzen ausgewertet werden, ohne dass dies von den teilnehmenden Personen bemerkt wird, was erhebliche Auswirkungen auf die Privatsphäre der Teilnehmenden hat. Bei der Auswertung von E-Mail-Kommunikation kann es passieren, dass hier unbeabsichtigt Daten offengelegt werden, die nur in einer Privatkommunikation verborgen bleiben sollten.
- Auch die Sicherheit der gespeicherten Daten kann durch Copilot berührt werden. Durch unberechtigte Abfragen der Nutzer besteht die Gefahr, dass geschützte Informationen offenbart werden,

wodurch Meldepflichten gem. DSGVO ausgelöst werden. Dies können auch Mandanten-/Kundendaten sein.

- Alle Nutzer sollten auf die Risiken des Copilot-Tools hingewiesen und sensibilisiert werden.
- Sie sollten Ihr Berechtigungskonzept überprüfen und klare Handlungsanweisungen zur Nutzung von Copilot verfassen.
- Beim Transkribieren von Teams-Calls benötigen Sie die Zustimmung der Teilnehmer.
- Sie sollten auch Ihren Datenschutzbeauftragten um die Durchführung einer Datenschutzfolgeabschätzung bitten.

Wenn ein Kunde die Aktivierung von Copilot Lizenzen wünscht, muss ein offiz. Weisungsbefugter des Kunden SPECTRUM in Textform (z.B. per E-Mail) bestätigen, dass man explizit die Microsoft-365-Einstellungen – trotz der datenschutzrechtlichen Risiken - geändert haben möchte, um Copilot aktivieren zu können.

Bestätigung an SPECTRUM:

Wir haben die Hinweise zu den datenschutzrechtlichen Risiken beim Einsatz von Microsoft Copilot gelesen und verstanden. Wir tragen die Verantwortung, dass unsere Mitarbeiter aufgeklärt und sensibilisiert werden. Hiermit wünschen wir ausdrücklich die Aktivierung der Microsoft Copilot Lizenz zu folgende Benutzer:

Kundenfirmierung: _____

Weisungsbefugter: _____

Ort, Datum: _____

An SPECTRUM per E-Mail an info@spectrum-news.de oder per Fax an 0211/695 60 2-99 schicken